16

Claims

1. A method for data transmission comprising the following
steps:

5

    - input first data from a stochastic process (114) into at
      least first and second users (102, 104; 402, 404; 502,
      504, 506, 508, 510, 512, 516) of a communication
      network (100, 106; 400, 406; 500, 514, 518),

10

    - in each of the at least first and second users: generate
      a symmetrical key (S1, S2) based on the first data and
      store the symmetrical key for the purpose of an
      encrypted data transmission between the at least first

15   and second users.

2. The method as claimed in claim 1, wherein the first data is
transmitted over the communication network (100, 106; 400, 406;
500, 514, 518).

20

3. The method as claimed in claim 1 or 2, wherein the first
data is obtained by acquisition of at least one measured value
from the stochastic process (114).

25   4. The method as claimed in claim 1, 2 or 3, wherein the
stochastic process is a time-variable parameter of an
automation system (500).

5. The method as claimed in one of the preceding claims 1 to 4,
30   wherein the first data is obtained from least significant bit
(LSB) positions of one or more measured values.

6. The method as claimed in one of the preceding claims 1 to 5, wherein each of the at least first and second users acquires stochastic data from which the first data is formed.

7. The method as claimed in claim 6, wherein the first data is formed from the stochastic data by means of a predefined combinatorial mechanism.

8. The method as claimed in claim 6 or 7, wherein the stochastic data is transmitted over the communication network (100, 106; 400, 406; 500, 514, 518).

9. The method as claimed in one of the preceding claims 1 to 8, wherein the symmetrical key is generated in the users at the request of a master user of the communication network.

10. The method as claimed in one of the preceding claims 1 to 9, wherein the symmetrical key is generated in the at least first and second users at predetermined times or after predetermined time intervals.

11. The method as claimed in one of the preceding claims 1 to 10, wherein the first data or the stochastic data is transmitted at a time of low utilization of the communication network.

12. The method as claimed in one of the preceding claims 1 to 11, wherein the first data or the stochastic data is transmitted using an asymmetrical encryption method.

13. The method as claimed in one of the preceding claims 1 to 12, wherein each of the at least first and second users has means (108; 408) for first and second encryption methods, with first and second symmetrical keys being generated in each case

based on the first data, and a changeover between the first and
second encryption methods being made in chronological sequence
for the encrypted data transmission.

5   14. The method as claimed in claim 13, wherein in order to
generate the first and second keys in each of the at least
first and second users, different first data is formed by
different combinatorial operations on the stochastic data.

10   15. A computer program product, in particular a digital memory
medium, having program means for performing the following
steps:

     - input first data from a stochastic process (114) into at
15   least first and second users (102, 104; 402, 404; 502,
504, 506, 508, 510, 512, 516) of a communication
network (100, 106; 400, 406; 500, 514, 518),

     - in each of the at least first and second users: generate
20   a symmetrical key (S1, S2) based on the first data and
store the symmetrical key for the purpose of an
encrypted data transmission between the at least first
and second users.

25   16. The computer program product as claimed in claim 15,
wherein the first data is obtained by acquisition of a measured
value from the stochastic process (114).

  17. The computer program product as claimed in claim 15 or 16,
30 wherein the first data is obtained from least significant bit
(LSB) positions of one or more measured values.

  18. A communication system having at least first and second
users (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516)

and a communication network (100, 106; 400, 406; 500, 514, 518) for the purpose of a data transmission between the at least first and second users, and having:

5   - means (112) for inputting first data from a stochastic process (114) into the at least first and second users,

       - in each of the at least first and second users: means (108; 408) for generating a symmetrical key based on

10   the first data and means (110; 426; 520, 522) for storing the symmetrical key for the purpose of an encrypted data transmission between the at least first and second users.

15   19. The communication system as claimed in claim 18, wherein the communication network (100, 106; 400, 406; 500, 514, 518) is a public network.

20. The communication system as claimed in claim 18 or 19,
20   wherein the communication network (100, 106; 400, 406; 500, 514, 518) is the internet and one user is embodied as a master user in order to initiate a key generation in the other users by transmission of a corresponding request via the internet.

25   21. The communication system as claimed in claim 18 or 19, wherein the communication network (100, 106; 400, 406; 500, 514, 518) is an Ethernet.

22. The communication system as claimed in claim 21, wherein
30   one of the users is embodied as a master user in order to output a command onto the Ethernet for the purpose of triggering the key generation in the users.

23. The communication system as claimed in one of the preceding claims 18 to 22, wherein the at least first and second users are components of an automation system (500).

5 24. The communication system as claimed in one of the preceding claims 18 to 23, wherein at least one of the users (516) is embodied for carrying out remote maintenance.